This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - Apple 'quicktime.qts' Error in Parsing 'qtif' Images Remote Denial of Service
  - Comersus Cart Multiple Vulnerabilities
  - DivX Player Skin File Directory Traversal
  - Funduc Search and Replace Buffer Overflow
  - Halocon Remote Denial of Service
  - INCA nProtect Gameguard Unauthorized Read/Write Access
  - KMiNT21 Software Golden FTP Server RNTO Command Buffer Overflow
  - Microsoft Internet Explorer Remote Information Disclosure
  - **Microsoft Windows Indexing Service Buffer Overflow (Updated)**
  - **Microsoft Windows ANI File Parsing Errors (Updated)**
  - **NodeManager SNMPv1 traps Buffer Overflow (Updated)**
  - Opera 'data:' URI Handler Spoofing
  - **Peer2Mail Password Disclosure (Updated)**
  - VLAIBB 'sig2dat' Integer Overflow & Remote Denial of Service
- UNIX / Linux Operating Systems
  - **Adobe Acrobat Reader mailListIsPdf() Buffer Overflow (Updated)**
  - ALSA Stack Protection Weakness
  - Apache Insecure Temporary File Creation
  - **Apache mod_ssl SSLCipherSuite Access Validation (Updated)**
  - **Apache mod_include Buffer Overflow (Updated)**
  - Apple Mac OS X 'at' Utility Information Disclosure
  - Apple Mac OS X Kernel searchfs() Buffer Overflow
  - Apple Mac OS X 'parse_machfile()' Denial of Service
  - Apple iSync mRouter Buffer Overflow
  - **ARJ Software UNARJ Remote Buffer Overflow (Updated)**
  - **Carsten Haitzler imlib Image Decoding Integer Overflow (Updated)**
  - Darwin Kernel Denial of Service
  - Ethereal Multiple Dissector Vulnerabilities
  - Fkey Remote Arbitrary File Disclosure
  - Gatos xatitv Buffer Overflow
  - **GD Graphics Library Remote Integer Overflow (Updated)**
  - GForge Directory Traversal
  - Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow
  - GNU Enscript Input Validation
  - GNU Queue Remote Buffer Overflows
  - **GNU a2ps Filenames Shell Commands Execution (Updated)**
  - **GNU ChBg simplify_path() Buffer Overflow (Updated)**
  - **GNU CUPS HPGL ParseCommand() Buffer Overflow (Updated)**
  - **GNU CUPS lppasswd Denial of Service (Updated)**
  - **GNU xine Buffer Overflow in pnm_get_chunk() (Updated)**
  - **GNU xine-lib Unspecified PNM and Real RTSP Clients Vulnerabilities (Updated)**
  - **ImageMagick Photoshop Document Buffer Overflow (Updated)**
  - Konversation IRC Client Multiple Remote Vulnerabilities
  - **LibTIFF Buffer Overflows (Updated)**
  - **Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory (Updated)**
  - **MPG123 Layer 2 Frame Header Buffer Overflow (Updated)**
  - Multiple Vendors PlayMidi Buffer Overflow
  - **Multiple Vendors LibTIFF TIFFDUMP Heap Corruption Integer Overflow (Updated)**
  - **Multiple Vendors LibXPM Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors glibc Buffer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges (Updated)**
  - Multiple Vendors Linux Kernel Audit Subsystem Denial of Service
  - Multiple Vendors Linux Kernel NFS I/O Denial of Service
  - **Multiple Vendors Linux Kernel Overlapping VMAs (Updated)**
  - **Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel SCSI IOCTL Integer Overflow (Updated)**
  - **Multiple Vendors Squid NTLM fakeauth_auth Helper Remote Denial of Service (Updated)**
  - **Open Group Motif / Open Motif libXpm Vulnerabilities (Updated)**
  - **Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities (Updated)**
  - SCO UnixWare 'CHRoot()' Feature Breakout
  - **Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow (Updated)**
  - SWORD 'diatheke.pl' Input Validation
  - **Todd Miller Sudo Restricted Command Execution BypasS (Updated)**
  - **Vim Insecure Temporary File Creation (Updated)**
  - **Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service (Updated)**
- Multiple Operating Systems
  - 3Com OfficeConnect Wireless 11g Access Point
  - Artifex Ghostscript Privilege Escalation
  - **AWStats Multiple Remote Input Validation (Updated)**
  - Cisco IOS Embedded Call Processing
  - Cool Coyote CoolForum Input Validation Vulnerabilities

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apple QuickTime	A remote Denial of Service vulnerability exists in the 'quicktime.qts' component when a specially crafted 'qtif' image file is created that contains an incomplete header. No workaround or patch available at time of publishing. An exploit has been published.	Apple 'quicktime.qts' Error in Parsing 'qtif' Images Remote Denial of Service	Low	SecurityTracker Alert, 1012991, January 25, 2005
Comersus Open Technologies Comersus Cart 6.0, 6.01	Multiple vulnerabilities exist: a vulnerability exists due to the incorrect removal of some installation files, which could let a remote malicious user obtain administrator access; a vulnerability exists in '/comersus/store/default.asp' due to insufficient sanitization of input passed to the 'Referer' header, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists in the 'comersus_supportError.asp' and 'comersus_backofficelite_supportError.asp' scripts due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.comersus.com/download.html A Proof of Concept exploit has been published.	Comersus Cart Multiple Vulnerabilities	High	SecurityTracker Alert, 1012989, January 25, 2005
DivX Player DivX Player 2.6	A Directory Traversal vulnerability exists when DPS '.dps', archive files are processed, which could let a remote malicious user obtain sensitive information and possibly execute arbitrary code. No workaround or patch available at time of publishing.	DivX Player Skin File Directory Traversal	Medium/ High (High if arbitrary	Securiteam, January 23, 2005

	A Proof of Concept exploit script has been published.		code can b executed)	
Funduc Software Search and Replace 5.0 & prior	A buffer overflow vulnerability exists when a zip folder is created that contains a specially crafted filename, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Funduc Search and Replace Buffer Overflow	High	SecurityTracker Alert, 1012990, January 25, 2005
Halocon Halocon 2.0.0.81	A remote Denial of Service vulnerability exists when a malicious user submits an empty UDP packet. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Halocon Remote Denial of Service	Low	Securiteam, January 17, 2005
INCA nProtect Gameguard	A vulnerability exists in the kernel driver functionality because the I/O permission mask can be modified, which could let an unauthorized malicious user obtain read/write access. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	INCA nProtect Gameguard Unauthorized Read/Write Access	Medium	Bugtraq, January 17, 2005
KMiNT21 Software Golden FTP Server Pro 2.05b & prior	A buffer overflow vulnerability exists when a specially crafted RNTO command is submitted, which could let a remote malicious user execute arbitrary code. Update available at: http://www.goldenftpserver.com/download.htm An exploit script has been published.	Golden FTP Server RNTO Command Buffer Overflow	High	Secunia Advisory, SA13966, January 24, 2005
Microsoft Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, preview, SP1&SP2, 6.0 SP1&SP2	A vulnerability exists due to a failure to secure scripts residing on a local computer, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit required.	Microsoft Internet Explorer Remote Information Disclosure	Medium	SecurityFocus, January 18, 2005
Microsoft Windows XP SP1 & prior service packs, 2003	A buffer overflow vulnerability exists in the Indexing Service due to the way query validation is handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-003.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Indexing Service Buffer Overflow CVE Name: CAN-2004-0897	Low/High (High if arbitrary code can be executed)	Microsoft Security Bulletin MS05-003, January 11, 2005 **US-CERT Vulnerability Note, VU#657118, January 20, 2005**
Microsoft Windows (XP SP2 is not affected)	A Denial of Service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx **Bulletin V1.1 (January 20, 2005): Updated CAN reference and added acknowledgment to finder for CAN-2004-1305.** **A Proof of Concept exploit script has been published.**	Microsoft Windows ANI File Parsing Errors CVE Name: CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Notes, VU#177584 & VU#697136, January 11, 2005 SecurityFocus, January 12, 2005 Technical Cyber Security Alert, TA05-012A, January 12, 2005 **Microsoft Security Bulletin, MS05-002, V1.1, January 20, 2005** **PacketStorm, January 25, 2005**
Mnet Soft Factor NodeManager Professional version 2.00	A buffer overflow vulnerability exists due to a boundary error when logging SNMPv1 traps, which could let a remote malicious user execute arbitrary code. Update available at: http://www.h4.dion.ne.jp/~you4707/NodeManagerPro.html **An exploit script has been published.**	NodeManager SNMPv1 Traps Buffer Overflow	High	Securiteam, January 18, 2005 **PacketStorm, January 19, 2005**

Opera Software Opera 5.x Opera 6.x Opera 7.x	A vulnerability exists due to an error in the processing of 'data:' URIs, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Opera 'data:' URI Handler Spoofing	High	US-CERT Vulnerability Note, VU#882926, January 21, 2005
peer2mail.com peer2mail 1.4 & prior	A vulnerability exists in the 'p2m.exe' process, which could let a malicious user obtain the password from memory. No workaround or patch available at time of publishing. **An exploit script has been published.**	Peer2Mail Password Disclosure	Medium	SecurityTracker Alert, 1012912, January 16, 2005 **PacketStorm, January 19, 2005**
VLAIBB sig2dat	Multiple vulnerabilities exist: an integer overflow vulnerability exists when a remote malicious user creates a specially crafted 'sig2dat' URL, which could lead to the execution of arbitrary code; and a remote Denial of Service vulnerability exists when a malicious user creates a specially crafted 'file:' parameter. No workaround or patch available at time of publishing. There is no exploit required; however, Proofs of Concept exploits have been published.	VLAIBB 'sig2dat' Integer Overflow & Remote Denial of Service	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1012920, January 19, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Adobe Adobe Acrobat Reader 5.0.9 for Unix	A buffer overflow vulnerability exists in in Adobe Acrobat Reader for Unix. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted PDF file that, when processed by the target user, will trigger a buffer overflow in the mailListIsPdf() function and execute arbitrary code. The code will run with the privileges of the target user. The vendor has issued a fixed version (5.0.10): http://www.adobe.com/support/techdocs/331153.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-12.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-674.html **SuSE: ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader mailListIsPdf() Buffer Overflow CVE Name: CAN-2004-1152	High	iDEFENSE Security Advisory 12.14.04 Gentoo Security Advisory, GLSA 200412-12 / acroread, December 16, 2004 Red Hat: RHSA-2004:674-07, December 23, 2004 SUSE Security Summary Report, SUSE-SR:2005:001, January 12, 2005 **US-Cert Vulnerability Note, VU#253024, January 24, 2005**
ALSA alsa-lib 1.0.6	A vulnerability exists in the Advanced Linux Sound Architecture (ALSA) library due to a weakness that disables stack protection schemes, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Currently we are not aware of any exploits for this vulnerability.	ALSA Stack Protection Weakness	High	Fedora Update Notification, FEDORA-2005-042, January 20, 2005
Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31-1.3.33	A vulnerability exists due to the creation of insecure temporary files, which could let a malicious user corrupt, write, or create arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache/ There is no exploit required.	Apache Insecure Temporary File Creation	Medium	SecurityFocus, January 19, 2005

Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesoft.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-562.html SuSE: In the process of releasing packages. RedHat: http://rhn.redhat.com/errata/RHSA-2004-600.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-010_RHSA-2004-600.pdf** **VMware:** **http://www.vmware.com/download/esx/** There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CVE Name: CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-21, October 22, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:122, November 2, 2004 Conectiva Linux Security Announcement, CLA-2004:885, November 4, 2004 Fedora Update Notification, FEDORA-2004-420, November 12, 2004 RedHat Security Advisory, RHSA-2004:562-11, November 12, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 RedHat Security Advisory, RHSA-2004:600-12, December 13, 2004 **Avaya Security Advisory, ASA-2005-010, January 14, 2005** **WMware Advisory, January 14, 2005**
Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.46, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31	A buffer overflow vulnerability exists in the 'get_tag()' function, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-03.xml Slackware: ftp://ftp.slackware.com/pub/slackware/s Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-600.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-010_RHSA-2004-600.pdf** Exploit scripts have been published.	Apache mod_include Buffer Overflow CVE Name: CAN-2004-0940	High	SecurityFocus, October 20, 2004 Slackware Security Advisory, SA:2004-305-01, November 1, 2004 Gentoo Linux Security Advisory, GLSA 200411-03, November 2, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:134, November 17,2004 Turbolinux Security Announcement, November 18, 2004 Red Hat Advisory: RHSA-2004:600-12, December 13, 2004 **Avaya Security Advisory, ASA-2005-010, January 14, 2005**
Apple Mac OS X 10.3-10.3.6, Mac OS X Server 10.3-10.3.6,	A vulnerability exists in the 'at' utility due to improper access controls on job schedule files, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit required; however, a Proof of Concept exploit has	Apple Mac OS X 'at' Utility Information Disclosure	Medium	Immunity Advisory, January 17, 2005

	been published.			
Apple Mac OS X 10.3-10.3.6, Mac OS X Server 10.3-10.3.6, Darwin Kernel 7.1	A buffer overflow vulnerability exists in the 'searchfs()' system call due to an error when calculating size arguments from user-controlled integer values, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Apple Mac OS X Kernel searchfs() Buffer Overflow	High	Immunity Advisory, January 17, 2005
Apple MacOSX 10.3.7 & prior	A Denial of Service vulnerability exists in 'bsd/kern/mach_loader.c' due to insufficient validation of the 'parse_machfile()' function. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X 'parse_machfile()' Denial of Service	Low	SecurityTracker Alert , 1012941, January 19, 2005
Apple Mac OS X 10.3.7 with iSync	A buffer overflow vulnerability exists in 'mRouter' when specially crafted options to the '-v' and '-a' command line switches are submitted, which could let a malicious user obtain root privileges. No workaround or patch available at time of publishing. An exploit script has been published.	Apple iSync mRouter Buffer Overflow	High	Securiteam, January 23, 2005
ARJ Software Inc. UNARJ 2.62-2.65	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied strings, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-29.xml SUSE: http://www.suse.de/de/security/2004_03_sr.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-007.html **Debian:** **http://security.debian.org/pool/updates/non-free/u/unarj/** Currently we are not aware of any exploits for this vulnerability.	ARJ Software UNARJ Remote Buffer Overflow CVE Name: CAN-2004-0947	High	SecurityTracker Alert I,: 1012194, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-29, November 19, 2004 SUSE Security Summary Report SUSE-SR:2004:003, December 7, 2004 Fedora Update Notification FEDORA-2004-414, December 11, 2004 RedHat Security Advisory, RHSA-2005:007-05, January 12, 2005 **Debian Security Advisory, DSA 652-1, January 21, 2005**
Carsten Haitzler imlib 1.x	Multiple vulnerabilities exist due to integer overflows within the image decoding routines. This can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library. Gentoo: http://security.gentoo.org/glsa/glsa-200412-03.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-651.html SUSE: http://www.suse.com/en/private/download/updates Debian: http://www.debian.org/security/2004/dsa-618 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imlib2/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **http://www.turbolinux.com/update/** Currently we are not aware of any exploits for these vulnerabilities.	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026 CAN-2004-1025	High	Secunia Advisory ID, SA13381, December 7, 2004 Red Hat Advisory, RHSA-2004:651-03, December 10, 2004 SecurityFocus, December 14, 2004 Debian DSA-618-1 imlib, December 24, 2004 Mandrakelinux Security Update Advisory, MDKSA-2005:007, January 12, 2005 **Turbolinux Security Announcement, January 20, 2005**

Darwin Darwin Kernel 7.1	A Denial of Service exists in 'mach-o loader' due to a failure to properly handle integer signedness. No workaround or patch available at time of publishing. An exploit script has been published.	Darwin Kernel Denial of Service	Low	Bugtraq, January 19, 2005
Ethereal Group Ethereal 0.8, 0.8.13-0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.8	Multiple vulnerabilities exist: remote Denial of Service vulnerabilities exist in the COPS, DLSw, DNP, Gnutella, and MMSE dissectors; and a buffer overflow vulnerability exists in the X11 dissector, which could let a remote malicious user execute arbitrary code. Ethereal: http://www.ethereal.com/download.html Debian: http://security.debian.org/pool/updates/main/e/ethereal/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-27.xml Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Dissector Vulnerabilities CVE Names: CAN-2005-0006 CAN-2005-0007 CAN-2005-0008 CAN-2005-0009 CAN-2005-0010 CAN-2005-0084	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert, 1012962, January 21, 2005
fkey fkey .1, .2	A vulnerability exists due to improper usage of local files by fkey, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been pulsed.	Fkey Remote Arbitrary File Disclosure	Medium	Securiteam, January 23, 2005
gatos gatos .5	A buffer overflow vulnerability exists in 'xutils.c' due to a boundary error in the 'exported_display()' function, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/g/gatos/ Currently we are not aware of any exploits for this vulnerability.	Gatos xatitv Buffer Overflow CVE Name: CAN-2005-0016	High	Secunia Advisory, : SA13884, January 17, 2005
GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28; **Avaya Converged Communications Server 2.0, Intuity LX Avaya MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing Avaya S8300 R2.0.1,R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0**	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml Debian: http://security.debian.org/pool/updates/main/libg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/libg/libgd/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-638.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-017_RHSA-2004-638.pdf** An exploit script has been published.	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990 CAN-2004-0941	High	Secunia Advisory, SA12996, October 28, 2004 Gentoo Linux Security Advisory, GLSA 200411-08, November 3, 2004 Ubuntu Security Notice, USN-21-1, November 9, 2004 Debian Security Advisories, DSA 589-1 & 591-1, November 9, 2004 Fedora Update Notifications, FEDORA-2004-411 & 412, November 11, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:132, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-25-1, November 16, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 Debian Security Advisories, DSA 601-1 & 602-1, November 29, 2004 Red Hat Advisory, RHSA-2004:638-09, December 17, 2004 **Avaya Security Advisory,**

				ASA-2005-017, January 18, 2005
GForge GForge 3.1-3.3, 3.21	A Directory Traversal vulnerability exists due to insufficient sanitization of the 'dir' parameter in 'controller.php' and the 'dire_name' parameter in 'controlleroo.php,' which could let a remote malicious user obtain sensitive information. Update available at: http://gforge.org/frs/?group_id=1 There is no exploit required.	GForge Directory Traversal	Medium	STG Security Advisory, SSA-20050120-24, January 20, 2005
Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Currently we are not aware of any exploits for this vulnerability.	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CVE Name: CAN-2005-0064	High	iDEFENSE Security Advisory, January 18, 2005
GNU Enscript 1.4, 1.5, 1.6, 1.6.1, 1.6.3, 1.6.4	Multiple vulnerabilities exist in 'src/util.c' and 'src/psgen.c': a vulnerability exists in EPSF pipe support due to insufficient input validation, which could let a malicious user execute arbitrary code; a vulnerability exists due to the way filenames are processed due to insufficient input validation, which could let a malicious user execute arbitrary code; and a Denial of Service vulnerability exists due to several buffer overflows. Debian: http://security.debian.org/pool/updates/main/e/enscript/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/e/enscript/ Currently we are not aware of any exploits for these vulnerabilities.	GNU Enscript Input Validation CVE Names: CAN-2004-1184 CAN-2004-1185 CAN-2004-1186	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID: 1012965, January 21, 2005
GNU Queue 1.x	Several buffer overflow vulnerabilities exist in 'queue.c' and 'queued.c,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/queue/ Currently we are not aware of any exploits for this vulnerability.	GNU Queue Remote Buffer Overflows CVE Name: CAN-2004-0555	High	Debian Security Advisory, DSA-643-1, January 18, 2005

GNU a2ps 4.13	A vulnerability exists that could allow a malicious user to execute arbitrary shell commands on the target system. a2ps will execute shell commands contained within filenames. A user can create a specially crafted filename that, when processed by a2ps, will execute shell commands with the privileges of the a2ps process. A patch for FreeBSD is available at: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/ print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain Debian: http://www.debian.org/security/2004/dsa-612 Gentoo: http://security.gentoo.org/glsa/glsa-200501-02.xml **OpenPKG:** **ftp://ftp.openpkg.org/release/** A Proof of Concept exploit has been published.	GNU a2ps Filenames Shell Commands Execution	High	SecurityTracker Alert ID, 1012475, December 10, 2004 Debian Security Advisory DSA-612-1 a2ps, December 20, 2004 Gentoo GLSA 200501-02, January 5, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.003, January 17, 2005**
GNU ChBg 1.5	A vulnerability was reported in ChBg. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ChBg scenario file that, when processed by the target user with ChBg, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the simplify_path() function in 'config.c.' FreeBSD is not affected because PATH_MAX is set to 1024, preventing the buffer overflow. **Debian:** **http://security.debian.org/pool/updates/main/c/chbg/** A Proof of Concept exploit script has been published.	GNU ChBg simplify_path() Buffer Overflow **CVE Name:** **CAN-2004-1264**	High	Secunia Advisory ID, SA13529, December 17, 2004 **Debian Security Advisory, DSA 644-1, January 18, 2005**
GNU CUPS 1.1.22	A vulnerability was reported in CUPS in the processing of HPGL files. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HPGL file that, when printed by the target user with CUPS, will execute arbitrary code on the target user's system. The code will run with the privileges of the 'lp' user. The buffer overflow resides in the ParseCommand() function in 'hpgl-input.c.' Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SGI:** **http://www.sgi.com/support/security/** A Proof of Concept exploit script has been published.	GNU CUPS HPGL ParseCommand() Buffer Overflow	High	CUPS Advisory STR #1023, December 16, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2005:008, January 17, 2005** **SGI Security Advisory, 20050101-01-U, January 19, 2005**
GNU CUPS lppasswd 1.1.22	A vulnerability was reported in the CUPS lppasswd utility. A local malicious user can truncate or modify certain files and cause Denial of Service conditions on the target system. There are flaws in the way that lppasswd edits the '/usr/local/etc/cups/passwd' file. Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-013.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SGI:** **http://www.sgi.com/support/security/** A Proof of Concept exploit has been published.	GNU CUPS lppasswd Denial of Service	Low	SecurityTracker Alert ID, 1012602, December 16, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2005:008, January 17, 2005** **SGI Security Advisory, 20050101-01-U, January 19, 2005**

GNU xine prior to 0.99.3	Multiple vulnerabilities exist that could allow a remote user to execute arbitrary code on the target user's system. There is a buffer overflow in pnm_get_chunk() in the processing of the RMF_TAG, DATA_TAG, PROP_TAG, MDPR_TAG, and CONT_TAG parameters. The vendor has issued a fixed version of xine-lib (1-rc8), available at: http://xinehq.de/index.php/releases A patch is also available at: http://cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/pnm.c?r1=1.20&r2=1.21 Conectiva: ftp://atualizacoes.conectiva.com.br/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-07.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** A Proof of Concept exploit has been published.	GNU xine Buffer Overflow in pnm_get_chunk() CVE Name: CAN-2004-1187 CAN-2004-1188	High	iDEFENSE Security Advisory 12.21.04 Gentoo, GLSA 200501-07, January 6, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005**
GNU xine-lib 1.x	Multiple vulnerabilities with unknown impacts exist due to errors in the PNM and Real RTSP clients. Update to version 1-rc8: http://xinehq.de/index.php/download Gentoo: http://security.gentoo.org/glsa/glsa-200501-07.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.	GNU xine-lib Unspecified PNM & Real RTSP Clients Vulnerabilities CVE Name: CAN-2004-1300	Not Specified	Secunia Advisory, SA13496, December 16, 2004 Gentoo Linux Security Advisory, GLSA 200501-07, January 6, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005**
ImageMagick ImageMagick 6.x	A buffer overflow vulnerability exists in 'coders/psd.c' when a specially crafted Photoshop document file is submitted, which could let a remote malicious user execute arbitrary code. Update available at: http://www.imagemagick.org/www/download.html **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/** **Debian: http://security.debian.org/pool/updates/main/i/imagemagick/** **Gentoo: http://security.gentoo.org/glsa/glsa-200501-26.xml** Currently we are not aware of any exploits for this vulnerability.	ImageMagick Photoshop Document Buffer Overflow **CVE Name: CAN-2005-0005**	High	iDEFENSE Security Advisory, January 17, 2005 **Ubuntu Security Notice, USN-62-1, January 18, 2005** **Debian Security Advisory, DSA 646-1, January 19, 2005** **Gentoo Linux Security Advisory, GLSA 200501-26, January 20, 2005**
Konversation IRC Client 0.15	Multiple vulnerabilities exist: a vulnerability exists in the 'Server::parseWildcards' function due to insufficient filtering of various parameters, which could let a remote malicious user execute arbitrary code; a vulnerability exists in certain Perl scripts if shell metacharacters in channel names or song names aren't properly quoted, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Quick Connection dialog because the password is used as the nickname, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://konversation.berlios.de/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-34.xml There is no exploit required; however, Proofs of Concept exploits have been published.	Konversation IRC Client Multiple Remote Vulnerabilities CVE Names: CAN-2005-0129 CAN-2005-0130 CAN-2005-0131	Medium/ High (High if arbitrary code can be executed)	Bugtraq, January 19, 2005

libtiff.org LibTIFF 3.6.1 Avaya MN100 (All versions), Avaya Intuity LX (version 1.1-5.x), Avaya Modular Messaging MSS (All versions)	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X: http://www.apple.com/swupdates/ Gentoo: KDE kfax: http://www.gentoo.org/security/en/glsa/glsa-200412-17.xml Avaya: No solution but workarounds available at: http://support.avaya.com/elmodocs2/security/ASA-2005-002_RHSA-2004-577.pdf **TurboLinux:** **http://www.turbolinux.com/update/** Proofs of Concept exploits have been published.	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004 Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 US-CERT Vulnerability Notes VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory, December 9, 2004 Apple Security Update SA-2004-12-02 Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004 Avaya Advisory ASA-2005-002, January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:914, January 6, 2005 **Turbolinux Security Announcement, January 20, 2005**
Linux Fedora RedHat SuSE Linux kernel 2.4 through 2.4.26, 2.6 through 2.6.7	A vulnerability exists in the Linux kernel in the processing of 64-bit file offset pointers thus allowing a local malicious user to view kernel memory. The kernel's file handling API does not properly convert 64-bit file offsets to 32-bit file offsets. In addition, the kernel provides insecure access to the file offset member variable. As a result, a local user can gain read access to large portions of kernel memory. Fedora: http://download.fedora.redhat.com/pub/	Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory CVE Name: CAN-2004-0415	High	ISEC Security Research, August 4, 2004 SGI Security Advisory, 20040804-01-U, August 26, 2004 Gentoo Linux Security Advisory GLSA 200408-24,

	fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/ SuSE: http://www.suse.de/de/security/2004_24_kernel.html Gentoo: http://security.gentoo.org/glsa/glsa-200408-24.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **VMware:** **http://www.vmware.com/download/esx/** A Proof of Concept exploit script has been published.			August 25, 2004 Mandrakelinux Security Update Advisory, August 26, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0041, August 9, 2004 Conectiva Linux Security Announcement, CLA-2004:879, October 26, 2004 **WMware Advisory, January 14, 2005**
mpg123 mpg123 0.59 m-0.59 s	A buffer overflow vulnerability exists when parsing frame headers for layer-2 streams, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200501-14.xml **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	MPG123 Layer 2 Frame Header Buffer Overflow CVE Name: CAN-2004-0991	High	Gentoo Linux Security Advisory, GLSA 200501-14, January 11, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:009, January 19, 2005**
Multiple Vendors MandrakeSoft Corporate Server 3.0, Linux Mandrake 10.0, AMD64, 10.1 X86_64, 10.1; Playmidi Linux Midi Player 2.4	A buffer overflow vulnerability exists in 'playmidi' due to insufficient validation of the 'main()' function, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/p/playmidi/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	PlayMidi Buffer Overflow CVE Name: CAN-2005-0020	High	Debian Security Advisory, DSA 641-1, January 17, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:010, January 19, 2005

Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux; LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6 .0, 3.6.1, 3.7, 3.7.1; RedHat Fedora Core2& Core 3; Ubuntu Ubuntu Linux 4.1 ppc, ia64, ia32	A vulnerability exists in the tiffdump utility, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/t/tiff/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-019.html **SGI:** **http://support.sgi.com/browse_request/linux_patches_by_os** **TurboLinux:** **http://www.turbolinux.com/update/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	LibTIFF TIFFDUMP Heap Corruption Integer Overflow CVE Name: CAN-2004-1183	High	SecurityTracker Alert ID, 1012785, January 6, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 **SGI Security Advisory, 20050101-01-U, January 19, 2005** **Turbolinux Security Announcement, January 20, 2005** **Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005**
Multiple Vendors Gentoo Linux; RedHat Fedora Core3, Core2; SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0; X.org X11R6 6.7 .0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1 4.3 .0	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information or cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200411-28.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE X.org: http://www.x.org/pub/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-537.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137 (libxpm) http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138 (XFree86) Debian: http://www.debian.org/security/2004/dsa-607 (XFree86) SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ **TurboLinux:** **http://www.turbolinux.com/update/**	Multiple Vendors LibXPM Multiple Vulnerabilities CVE Name: CAN-2004-0914	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	X.Org Foundation Security Advisory, November 17, 2004 Fedora Update Notifications, FEDORA-2004-433 & 434, November 17 & 18, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004 Fedora Security Update Notifications FEDORA-2003-464, 465, 466, & 467, December 1, 2004 RedHat Security Advisory, RHSA-2004:537-17, December 2, 2004 Mandrakesoft: MDKSA-2004:137: libxpm4; MDKSA-2004:138: XFree86, November 22, 2004 Debian Security Advisory DSA-607-1 xfree86 -- several vulnerabilities, December 10, 2004 **Turbolinux Security Announcement, January 20, 2005**

	Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors glibc 2.2	A buffer overflow vulnerability exists in the resolver libraries of glibc 2.2. SUSE: ftp://ftp.SUSE.com/pub/SUSE Red Hat: http://rhn.redhat.com/errata/ RHSA-2004-586.html Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:159 **Avaya:** **http://support.avaya.com/** **elmodocs2/security/** **ASA-2005-011_RHSA-2004-586.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors glibc Buffer Overflow CVE Name: CAN-2002-0029 CAN-2004-0968	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004 Red Hat RHSA-2004:586-15, December 20, 2004 Mandrakesoft, MDKSA-2004:159, December 29, 2004 **Avaya Security Advisory, ASA-2005-011, January 14, 2005**
Multiple Vendors Linux kernel 2.2-2.2.2.27 -rc1, 2.4-2.4.29 -rc1, 2.6 .10, 2.6- 2.6.10	A race condition vulnerability exists in the page fault handler of the Linux Kernel on symmetric multiprocessor (SMP) computers, which could let a malicious user obtain superuser privileges. Fedora: http://download.fedora.redhat.com/pub/f edora/linux/core/updates/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** **RedHat:** **http://rhn.redhat.com/errata/** **RHSA-2005-016.html** **http://rhn.redhat.com/errata/** **RHSA-2005-017.html** Exploit scripts have been published.	Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges CVE Name: CAN-2005-0001	High	SecurityTracker Alert, 1012862, January 12, 2005 **SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005** **RedHat Security Advisory, RHSA-2005:016-13 & 017-14, January 21, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2, 2.6 -test1-test11, 2.6-2.6.10, 2.6.10 rc1; RedHat Desktop 3.0, Enterprise Linux WS 3, Linux ES 3, Linux AS 3; S.u.S.E. Linux 8.1, 8.2, 9.0-9.2, Linux Desktop 1.0, Linux Enterprise Server 9, 8, Novell Linux Desktop 9.0	A Denial of Service vulnerability exists in the audit subsystem of the Linux kernel. . RedHat: http://rhn.redhat.com/errata/ RHSA-2005-043. SuSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Audit Subsystem Denial of Service CVE Name: CAN-2004-1237	Low	RedHat Security Advisory, RHSA-2005:043-13, January 18, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.28, 2.4.29rc1&rc2, 2.5 .0-2.5.69, 2.6 -test1-test11, 2.6-2.6.10; SuSE . Linux 8.1, 8.2, 9.0	A Denial of Service vulnerability exists with Direct I/O access to NFS file systems. SuSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel NFS I/O Denial of Service	Low	SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005
Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2	A vulnerability exists in the processing of ELF binaries on IA64 systems due to improper checking of overlapping virtual memory address allocations, which could let a malicious user cause a Denial of Service or potentially obtain root privileges. Patch available at: http://linux.bkbits.net:8080/linux-2.6/cset@ 41a6721cce-LoPqkzKXudYby_3TUmg Trustix:	Linux Kernel Overlapping VMAs CVE Name: CAN-2005-0003	Low/High (High if root access can be obtained)	Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 **RedHat Security Advisories, RHSA-2005:043-13 & RHSA-2005:017-14m January 18 & 21, 2005**

	ftp://ftp.trustix.org/pub/trustix/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-043.html** **http://rhn.redhat.com/errata/RHSA-2005-017.html** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32; SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html RedHat: http://rhn.redhat.com/errata/RHSA-2004-504.html http://rhn.redhat.com/errata/RHSA-2004-505.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for these vulnerabilities	Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service CVE Names: CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 Ubuntu Security Notice, USN-39-1, December 16, 2004 RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004 **SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005**
Multiple Vendors Linux Kernel 2.6 .10, 2.6, test-test11, 2.6.1-2.6.10, 2.6.10 rc2; RedHat Fedora Core2&3	An integer overflow vulnerability exists in the 'scsi_ioctl.c' kernel driver due to insufficient sanitization of the 'sg_scsi_ioctl' function, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SCSI IOCTL Integer Overflow	High	Bugtraq, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 **SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005**
Multiple Vendors Squid 2.x; **Gentoo Linux;Ubuntu Linux 4.1 ppc, ia64, ia32**	A remote Denial of Service vulnerability exists in the NTLM fakeauth_auth helper when running under a high load or for a long period of time, and a specially crafted NTLM type 3 message is submitted. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-fakeauth_auth.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM fakeauth_auth Helper Remote Denial of Service	Low	Secunia Advisory, SA13789, January 11, 2005 Gentoo Linux Security Advisor, GLSA 200501-25, January 17, 2005 **Ubuntu Security Notice, USN-67-1, January 20, 2005**

Open Group Open Motif 2.x, Motif 1.x	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-537.html Gentoo: http://security.gentoo.org/glsa/glsa-200410-09.xml Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/x/xfree86/ **TurboLinux:** **http://www.turbolinux.com/update/** Currently we are not aware of any exploits for these vulnerabilities.	Open Group Motif / Open Motif libXpm Vulnerabilities CVE Names: CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Solutions Secunia Advisory ID: SA13353, December 2, 2004 RedHat Security Advisory: RHSA-2004:537-17, December 2, 2004 **Turbolinux Security Announcement, January 20, 2005**
Remote Sensing LibTIFF 3.5.7, 3.6.1, 3.7.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-019.html **SGI:** **http://support.sgi.com/browse_request/linux_patches_by_os** **TurboLinux:** **http://www.turbolinux.com/update/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CVE Name: CAN-2004-1308	High	iDEFENSE Security Advisory 12.21.04 Secunia SA13629, December 23, 2004 SUSE Security Announcement, SUSE-SA:2005:001, January 10, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 US-Cert Vulnerability Note, VU#125598, January 14, 2005 **SGI Security Advisory, 20050101-01-U, January 19, 2005** **Turbolinux Security Announcement, January 20, 2005** **Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005**
SCO Unixware 7.1.1, 7.1.3, 7.1.4	A vulnerability exists in the 'chroot()' feature due to errors in the implementation, which could let a malicious user break out of the chroot restriction and access arbitrary files.	SCO UnixWare 'CHRoot()' Feature Breakout	Medium	SCO Security Advisory, SCOSA-2005.2, January 14, 2005

	Patches available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.2 An exploit script has been published.	CVE Name: CAN-2004-1124		
Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 .STABLE4&5, 2.4 .STABLE6&7, 2.4 .STABLE2, 2.4, 2.5 .STABLE3-7, 2.5 .STABLE1	Two vulnerabilities exist: remote Denial of Service vulnerability exists in the Web Cache Communication Protocol (WCCP) functionality due to a failure to handle unexpected network data; and buffer overflow vulnerability exists in the 'gopherToHTML()' function due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-wccp_denial_of_service.patch http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-gopher_html_parsing.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml **Debian:** **http://security.debian.org/pool/updates/main/s/squid/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/squid/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit required.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow **CVE Names:** **CAN-2005-0094** **CAN-2005-0095**	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA13825, January 13, 2005 **Debian Security Advisory, DSA 651-1, January 20, 2005** **Ubuntu Security Notice, USN-67-1, January 20, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:014, January 25, 2005**
The SWORD Project SWORD 1.5.3	A vulnerability exists in 'diatheke.pl' due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/s/sword/ There is no exploit required.	SWORD 'diatheke.pl' Input Validation CVE Name: CAN-2005-0015	High	Debian Security Advisory, DSA 650-1, January 20, 2005
Todd Miller Sudo 1.5.6-1.5.9, 1.6-1.6.8	A vulnerability exists due to an error in the environment cleaning, which could let a malicious user execute arbitrary commands. Patch available at: http://www.courtesan.com/sudo/download.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/ Debian: http://security.debian.org/pool/updates/main/s/sudo/ **OpenPKG:** **ftp://ftp.openpkg.org/release/** There is no exploit code required.	Sudo Restricted Command Execution Bypass	High	Secunia Advisory, SA13199, November 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:133, November 15, 2004 Trustix Secure Linux Security Advisories, TSLSA-2004-0058 & 061, November 16 & 19, 2004 Ubuntu Security Notice, USN-28-1, November 17, 2004 Debian Security Advisory, DSA 596-1, November 24, 2004 **OpenPKG Security Advisory, OpenPKG-SA-2005.002, January 17, 2005**
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/v/vim/** There is no exploit required.	Vim Insecure Temporary File Creation **CVE Name:** **CAN-2005-0069**	Medium	Secunia Advisory, SA13841, January 13, 2005 **Ubuntu Security Notice, USN-61-1, January 18, 2005**

Yukihiro Matsumoto Ruby 1.8.x	A remote Denial of Service vulnerability exists due to an input validation error in 'cgi.rb.' Debian: http://security.debian.org/pool/updates/main/r/ruby Mandrake: http://www.mandrakesoft.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/l Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-23.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-635.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-635.html** Currently we are not aware of any exploits for this vulnerability.	Yukihiro Matsumoto Ruby Infinite Loop Remote Denial of Service CVE Name: CAN-2004-0983	Low	Secunia Advisory, SA13123, November 8, 2004 Ubuntu Security Notice, USN-20-1, November 9, 2004 Fedora Update Notification, FEDORA-2004-402 & 403, November 11 & 12, 2004 Gentoo Linux Security Advisory, GLSA 200411-23, November 16, 2004 Red Hat Advisory, RHSA-2004:635-03, December 13, 2004 **RedHat Security Advisory, RHSA-2004:635-06, January 17, 2005** **SGI Security Advisory, 20050101-01-U, January 19, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
3Com OfficeConnect Wireless 11g Access Point Access Vulnerability prior to firmware version 1.03.07A	An access vulnerability exists that could allow a remote malicious user to obtain sensitive information from the router, including the password and the encryption key. A remote user can send a special URL to the web administration port on port 80 to obtain sensitive information. Fixed firmware (1.03.07A for 3CRWE454G72), is available at: http://www.3com.com/products/en_US/result.jsp?selected=6&sort=effdt&order=desc&sku=3CRWE454G72 A Proof of Concept exploit has been published.	3Com OfficeConnect Wireless 11g Access Point CVE Name: CAN-2005-0112	High	iDEFENSE Security Advisory 01.20.05
Artifex Software Ghostscript 8.01 and 8.50	Multiple vulnerabilities exist due to scripts creating temporary files insecurely. This can be exploited by local users to create or overwrite arbitrary files on the system with the privileges of the user running a vulnerable script. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Artifex Ghostscript Privilege Escalation	Medium	January 21, 2005
AWStats AWStats 5.0-5.9, 6.0-6.2	Several vulnerabilities exist: a vulnerability exists in the 'awstats.pl' script due to insufficient validation of the 'configdir' parameter, which could let a remote malicious user execute arbitrary code; and an unspecified input validation vulnerability exists. Upgrades available at: http://awstats.sourceforge.net/files/awstats-6.3.tgz **An exploit script has been published.**	AWStats Multiple Remote Input Validation	High	Securiteam, January 18, 2005 **PacketStorm, January 25, 2005**
Cisco Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony	A vulnerability exists in some Cisco products in processing certain malformed control protocol messages that may cause a reload of the device and a Denial of Service. Vendor solution available at: http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Embedded Call Processing	Low	Cisco Security Advisory, Document ID: 63708, January 19, 2005 US-CERT VU#613384, January 21, 2005

Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST)				
Cool Coyote CoolForum 0.7.2 beta	An input validation vulnerability exists that could permit a remote malicious user to conduct Cross-Site Scripting attacks and a remote administrative user to inject SQL commands. Certain input fields such as the 'email' parameter of the 'mail.php' script are not validated. A fixed version (0.7.3) is available at: http://www.coolforum.net/index.php?p=dlcoolforum A Proof of Concept exploit has been published.	Cool Coyote CoolForum Input Validation Vulnerabilities	High	SecurityTracker Alert ID: 1012985, January 25, 2005
DataRescue IDA Pro 4.6 Service Pack 1 and 4.7	A vulnerability exists due to a boundary error when parsing the PE (Portable Executable) import directory. This can be exploited to cause a stack-based buffer overflow. This may allow execution of arbitrary code when the malicious PE file is opened. The vendor has issued a temporary fix: http://www.datarescue.be/freefiles/ida47vfix.zip Currently we are not aware of any exploits for this vulnerability.	DataRescue IDA Pro Remote Execution	High	iDEFENSE Security Advisory 01.24.05
GNU Siteman 1.1.9	An authentication vulnerability exists that could permit a remote malicious user to gain administrative access by sending a special HTTP POST request to the 'users.php' script to add a user with administrative privileges. No workaround or patch available at time of publishing. Exploit scripts have been published.	GNU Siteman Escalated Privilege	High	SecurityTracker Alert ID: 1012951, January 20, 2005
GNU TikiWiki versions prior to 1.8.5 and 1.9 DR4	Multiple vulnerabilities exist due to missing validation of files placed in the 'temp' directory. This can be exploited to execute arbitrary PHP scripts. Update to version 1.8.5: http://sourceforge.net/project/showfiles.php?group_id=64258 Currently we are not aware of any exploits for this vulnerability.	GNU TikiWiki Remote Code Execution	High	TikiWiki January Security Alert, January 16, 2005
HARTEG IT CMSimple prior to 2.4 beta 5	An input validation vulnerability exists that could permit a remote malicious user to conduct Cross-Site Scripting attacks. The search and guestbook components do not properly validate user-supplied input to filter HTML code. Update to beta version (2.4 beta 5), available at: http://www.cmsimple.dk/?Downloads:Beta_version Currently we are not aware of any exploits for this vulnerability.	HARTEG IT CMSimple Input Validation	High	SecurityTracker Alert ID: 1012926, January 18, 2005
ITA Forum ITA Forum 1.49	Multiple SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input before used in SQL queries, which could let a remote malicious user compromise the application, or obtain/modify data. No workaround or patch available at time of publishing. An exploit script has been published.	ITA Forum Multiple SQL Injection	Medium	SecurityFocus, January 18, 2005
KLDP JSBoard 2.0.9 and prior	An input validation vulnerability exists in the 'session.php' script that could permit a remote malicious user to view arbitrary files. The script does not properly validate the user-supplied 'table' variable. Update to fixed version (2.0.10), available at: http://kldp.net/frs/download.php/1729/jsboard-2.0.10.tar.gz A Proof of Concept exploit has been published.	KLDP JSBoard 'session.php' Input Validation	Medium	STG Security January 20, 2005
MercuryBoard MercuryBoard 1.1.1	Multiple vulnerabilities exist that could permit a remote user to conduct Cross-Site Scripting attacks and determine the installation path. These vulnerabilities are due to errors in the 'func/pm.php' script, the 'func/members.php' function, and the 'global.php' script. Update to version (1.1.2), available at: http://www.mercuryboard.com/index.php?a=downloads Currently we are not aware of any exploits for these vulnerabilities.	MercuryBoard Cross-Site Scripting & Path DIsclosure	High	SecurityTracker Alert ID: 1012984, January 25, 2005
MPM PHP Scripts Guestbook 1.2, 1.5	A vulnerability exists in 'top.php' due to insufficient verification of the 'header' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script has been published.**	MPM Guestbook 'top.php' Input Validation	High	SYSTEMSECURE.ORG Advisory, January 13, 2005 **PacketStorm, January 25, 2005**

Multiple Vendors Check Point Software FireWall-1 R55 HFA08 with SmartDefense; Internet Security Systems SiteProtector 2.0.4.561, 2.0 SP3; IronPort IronPort with Sophos AV Engine 3.88; McAfee Webshield 3000 4.3.20; TippingPoint Unity-One with Digital Vaccine 2.0.0.2070; Trend Micro InterScan Messaging Security Suite 3.81, 5.5, Trend Micro WebProtect 3.1	A security vulnerability exists due to a failure to decode base64-encoded images in 'data' URIs, which could lead to a false sense of security. **TippingPoint:** **https://tmc.tippingpoint.com/TMC** There is no exploit required.	Multiple Vendor Anti-Virus GatewayBase64 Encoded Image Decode Failure	Medium	Bugtraq, January 11, 2005 **SecurityFocus, January 18, 2005**
MySQL MaxDB prior to 7.5.0.21	Multiple vulnerabilities exist that could cause a Denial of Service in the MaxDB Web Agent. A remote malicious user can submit a HTTP request with invalid parameters to trigger a NULL pointer dereference in the sapdbwa_GetUserData() function in the webdav handler code. A remote user can also send an HTTP request with special HTTP headers to trigger another error. SAP DB Web Agent is also affected. Update available at: http://dev.mysql.com/downloads/maxdb/7.5.00.html Currently we are not aware of any exploits for these vulnerabilities.	MySQL MaxDB Denial of Service	Low	iDEFENSE, Security Advisory 01.19.05
MySQL MySQL 4.x	A vulnerability exists in the 'mysqlaccess.sh' script because temporary files are created in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://lists.mysql.com/internals/20600 **Ubuntu:** **http://www.ubuntulinux.org/support/documentation/usn/usn-63-1** **Debian:** **http://www.debian.org/security/2005/dsa-647** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200501-33.xml** Currently we are not aware of any exploits for this vulnerability.	MySQL 'mysqlaccess.sh' Unsafe Temporary Files CVE Name: CAN-2005-0004	Medium	SecurityTracker Alert, 1012914, January 17,2005 **Ubuntu Security Notice USN-63-1 January 18, 2005** **Debian Security Advisory DSA-647-1 mysql, January 19, 2005** **Gentoo GLSA 200501-33, January 23, 2005**
Netegrity SiteMinder	A Cross-Site Scripting vulnerability exists in 'smpwservicescgi.exe' that could allow a remote malicious user to conduct spoofing/phishing attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netegrity SiteMinder Cross-Site Scripting	High	SecurityTracker Alert ID: 1012927, January 18, 2005
Netscape Navigator 7.2	Netscape Navigator is prone to a vulnerability that may result in a browser crash. This issue is exposed when the browser performs an infinite JavaScript array sort operation. It is conjectured that this will only result in a Denial of Service and is not further exploitable to execute arbitrary code, though this has not been confirmed. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netscape Navigator Denial of Service	Low	SecurityFocus, Bugtraq ID 12331, January 21, 2005
Novell GroupWise WebAccess	Two vulnerabilities exist that could permit a remote malicious user to bypass the authentication mechanism using a specially crafted URL. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Novell GroupWise WebAccess Authentication Bypass	High	SecurityFocus Bugtraq ID 12310, January 19, 2005

Oracle Oracle Database 10g Release 1, versions 10.1.0.2, 10.1.0.3 and 10.1.0.3.1; Oracle9i Database Server Release 2, versions 9.2.0.4, 9.2.0.5 and 9.2.0.6; Oracle9i Database Server Release 1, versions 9.0.1.4, 9.0.1.5 and 9.0.4 (9.0.1.5 FIPS); Oracle8i Database Server Release 3, version 8.1.7.4; Oracle8 Database Release 8.0.6, version 8.0.6.3; Oracle Application Server 10g Release 2 (10.1.2); Oracle Application Server 10g (9.0.4), versions 9.0.4.0 and 9.0.4.1; Oracle9i Application Server Release 2, versions 9.0.2.3 and 9.0.3.1; Oracle9i Application Server Release 1, version 1.0.2.2; Oracle Collaboration Suite Release 2, version 9.0.4.2; Oracle E-Business Suite and Applications Release 11i (11.5); Oracle E-Business Suite and Applications Release 11.0	Twenty-three vulnerabilities exist in various Oracle products that are corrected in the Oracle January 2005 patch update. These vulnerabilities are as follows: 1) A boundary vulnerability exists in the Networking component that can be exploited to cause a Denial of Service. 2) An unspecified vulnerability exists in the LOB Access component that can be exploited to disclose sensitive information. 3) An unspecified vulnerability exists in the Spatial component that can be exploited to disclose information, manipulate data, or cause a Denial of Service. 4) An unspecified vulnerability exists in the UTL_FILE component that can be exploited to manipulate information. 5) An unspecified vulnerability exists in the Diagnostic component that can be exploited to disclose information, manipulate data, or cause a Denial of Service. 6) An unspecified vulnerability exists in the XDB component that can be exploited to disclose or manipulate information. 7+8) Two unspecified vulnerabilities exists in the XDB component that can be exploited to disclose or manipulate information. 9) An unspecified vulnerability exists in the Dataguard component that can be exploited to disclose or manipulate information. 10) An unspecified vulnerability exists in the Log Miner component that can be exploited to disclose or manipulate information. 11) An unspecified vulnerability exists in the OLAP component can potentially be exploited to disclose or manipulate information. 12) An unspecified vulnerability exists in the Data Mining component that can be exploited to disclose or manipulate information. 13) An unspecified vulnerability exists in the Advanced Queuing component that can be exploited to disclose or manipulate information. 14) An unspecified vulnerability exists in the Change Data Capture component that can be exploited to disclose or manipulate information. 15) An unspecified vulnerability exists in the Change Data Capture component can potentially be exploited to disclose or manipulate information. 16) An unspecified vulnerability exists in the Database Core component that can be exploited to disclose or manipulate information. 17) An unspecified vulnerability exists in the OHS component that can be exploited to disclose or manipulate information. 18) An unspecified vulnerability exists in the Report Server component that can be exploited to disclose or manipulate information. 19) An unspecified vulnerability exists in the Forms component that can be exploited to cause a Denial of Service. 20) An unspecified vulnerability exists in the mod_plsql component that can be exploited to disclose or manipulate information. 21) An unspecified vulnerability exists in the Calendar component that can be exploited to disclose information, manipulate data, or cause a Denial of Service by viewing a malicious image. 22, 23) Two vulnerabilities exists in Oracle E-Business Suite that can be exploited to disclose or manipulate information. Apply updates listed in vendor advisory: http://otn.oracle.com/deploy/security/pdf/cpu-jan-2005_advisory.pdf Currently we are not aware of any exploits for these vulnerabilities.	Oracle Multiple Vulnerabilities	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained or manipulated; and High if arbitrary code can be executed)	Oracle Patch Update January 2005
PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute	PHP Multiple Remote Vulnerabilities CVE Names: CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004 Conectiva Linux Security Announcement, CLA-2005:915, January 13, 2005 **Red Hat, Advisory: RHSA-2005:031-08,**

	arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' if not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-031.html** **SuSE: ftp://ftp.suse.com/pub/suse/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	CAN-2004-1065		**January 19, 2005** **SUSE Security Announcement, SUSE-SA:2005:002, January 17, 2005** **Ubuntu Security Notice, USN-66-1, January 20, 2005**
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass	Medium	SecurityTracker Alert ID, 1011984, October 28, 2004 **Ubuntu Security Notice, USN-66-1, January 20, 2005**
Research in Motion Blackberry Enterprise Server for Domino 2.1 SP2 through 4.0; Blackberry Enterprise Server for Exchange 2.1 through 4.0 SP1	A remote Denial of Service vulnerability exists due to an error while processing WML (Wireless Markup Language) pages in the 'Mobile Data Service'. Upgrade to Blackberry Enterprise Server for Domino 2.2 Service Pack 4 Hot Fix 2 or Blackberry Enterprise Server for Exchange 3.6 Service Pack 4 Hot Fix 2 available at: http://www.blackberry.com/support/downloads/hot_fixes.shtml Currently we are not aware of any exploits for this vulnerability.	Research in Motion Blackberry Enterprise Server Mobile Data Service Denial of Service	Low	BlackBerry Enterprise Server for IBM Lotus Domino Version 2.2.4 Hot fix 2 and BlackBerry Enterprise Server for Microsoft Exchange Version 3.6 Service Pack 4 Hot Fix 2 Release Notes
sightid BRIBBLE prior to 1.5.35	A vulnerability exists due to an error in the webadmin authentication process and can be exploited to bypass security restrictions without a valid password. Update to version 1.5.35: http://sourceforge.net/project/showfiles.php?group_id=94803 Currently we are not aware of any exploits for this vulnerability.	sightid BRIBBLE Access	Medium	Secunia, SA13976, January 25, 2005
Sun Sun Java SDK 1.4.x, Sun Java SDK 1.3.x, Sun Java JRE 1.4.x, Sun Java JRE 1.3.x	Two vulnerabilities exists which can be exploited to bypass certain security restrictions or compromise a user's system. The first vulnerability involves an error in the Java Plug-in within the handling of JavaScript calling into Java code can be exploited by a malicious applet hosted on a web site to access and modify local files or execute local applications. This vulnerability has been fixed in SDK / JRE 1.4.2_01 and later, and SDK / JRE 1.3.1_13 and later. The second vulnerability involves an error in the way applets on the same web page can interfere with each other can be exploited to load files and web pages in another applet. This vulnerability has been fixed in SDK / JRE 1.4.2_06 and later, and SDK / JRE 1.3.1_13 and later. For both vulnerabilities, JDK and JRE 5.0 are not affected. Updates available in advisory: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57708-1 Currently we are not aware of any exploits for these vulnerabilities.	Sun Java Plug-In Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Sun Alert ID: 57708, January 18, 2005
Sybari AntiGen 7.x	Multiple vulnerabilities exist due to input validation and boundary errors that can be exploited to cause a Denial of Service and allow malware to bypass the software. Update to version 7.0 SR5 for Domino, build 745, available at: http://www.sybari.com/ Currently we are not aware of any exploits for these vulnerabilities.	Sybari AntiGen for Domino Multiple Vulnerabilities	Low	SecurityFocus, Bugtraq ID 12323, January 20, 2005

Veritas Software NetBackup BusinesServer 3.4, 3.4.1, 4.5, NetBackup DataCenter 3.4, 3.4.1, 4.5, NetBackup Enterprise Server 5.1, NetBackup Server 5.0, 5.1	A input validation vulnerability exists in the 'bpjava-susvc' process used for administration, which could let a remote authenticated malicious user execute commands with root privileges. The vendor has described a configuration workaround available at: http://support.veritas.com/docs/271727 Currently we are not aware of any exploits for this vulnerability.	VERITAS NetBackup Input	High	SecurityTracker Alert, 1011863, October 21, 2004 **US-CERT, #VU#685456, January 18, 2005**
Wikimedia Foundation MediaWiki 1.4 beta - 1.4beta4	An input validation vulnerability exists in 'setup.php' that could permit a remote user to execute arbitrary PHP code on the target system. A fixed version of the 1.4 beta series (1.4beta5), available at: http://zwinger.wikimedia.org/mediawiki/mediawiki-1.4beta5.tar.gz Currently we are not aware of any exploits for this vulnerability.	Wikimedia MediaWiki Input Validation	High	SecurityFocus Bugtraq ID 12305, January 18, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
January 25, 2005	awexpl.c GHCaws.pl	Yes	Exploits for the AWStats Multiple Remote Input Validation vulnerabilities.
January 25, 2005	crafted.c	No	Script that exploits the Funduc Search and Replace Buffer Overflow vulnerability.
January 25, 2005	gbook.tgz	No	Exploit for the MPM Guestbook 'top.php' Input Validation vulnerability.
January 25, 2005	HOD-ms05002-ani-expl.c	Yes	Proof of Concept exploit for the Microsoft Windows ANI File Parsing Errors vulnerability.
January 25, 2005	siteman.pl.txt siteman.pl siteman	No	Exploits for the GNU Siteman Escalated Privilege vulnerability.
January 23, 2005	fm-iSink.c	No	Script that exploits the Apple iSync mRouter Buffer Overflow vulnerability.
January 22, 2005	ethereal-0.10.9.tar.gz	N/A	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
January 22, 2005	goldenftpserver.pl goldenSploit.pl	Yes	Perl scripts that exploit the Golden FTP Server RNTO Command Buffer Overflow vulnerability.
January 21, 2005	divxplayerbug.dps	No	Proof of Concept exploit for the DivX Player Skin File Directory Traversal vulnerability.
January 19, 2005	CDBFP.zip	N/A	Remote fingerprinting tool for Oracle and DB2 that allows for discovery of versions and OS information.
January 19, 2005	demgrPOC.cpp	Yes	Exploit for the NodeManager SNMPv1 Traps Buffer Overflow vulnerability.
January 19, 2005	fm-nacho.c	No	Denial of Service exploit for the Darwin Kernel Mach File Parsing Local Integer Overflow vulnerability.
January 19, 2005	peer2mail.c	No	Script that exploits the Peer2Mail Password Disclosure vulnerability.
January 19, 2005	tcpick-0.2.1.tar.gz	N/A	A textmode sniffer that can track TCP streams and saves the data captured in files or displays them in the terminal.
January 19, 2005	xfkey.c	No	Script that exploits the Fkey Remote Arbitrary File Disclosure vulnerability.
January 18, 2005	libexploit	Yes	Script that exploits the SCO UnixWare 'CHRoot()' Feature Breakout vulnerability.
January 18, 2005	macosx_kernel.c	No	Proof of Concept exploit for the Mac OS X Kernel searchfs() Buffer Overflow vulnerability.
January 17, 2005	lithsock.zip	No	Proof of Concept exploit for the Halocon Remote Denial of Service vulnerability.
January 17, 2005	NPPTNT2Access.cpp	No	Proof of Concept exploit for the INCA nProtect Gameguard Unauthorized Read/Write Access vulnerability.
January 17, 2005	rf54ita.pl	No	Perl script that exploits the ITA Forum Multiple SQL Injection vulnerabilities.

[back to top]

Trends

- New ways to trick consumers into revealing passwords, bank account number, etc are being developed that make Internet 'phishing' scams are becoming more difficult to detect. the use of worms and spyware to divert consumers to fraudulent sites has increased. For more information, see: "Internet 'Phishing' Scams

Getting More Devious" at http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=7372770.

- People using wireless high-speed net (wi-fi) are being warned about fake hotspots, or access points because the fake hotspots are actually unauthorized base stations. This threat has been nicknamed evil twins. Once a user is logged onto an Evil Twin, sensitive data can be intercepted.

  TOP 10 WI-FI COUNTRIES FOR HOTSPOTS

  - United States 22,081
  - United Kingdom 9,356
  - Germany 5,713
  - France 3,239
  - Japan 2,197
  - Switzerland 1,311
  - Italy 1,111
  - Spain 1,073
  - Canada 826
  - Australia 800

  For more information, see: 'Evil twin' fear for wireless net' at: http://news.bbc.co.uk/1/hi/technology/4190607.stm.

- According to a new poll released by WatchGuard Technologies, IT professionals consider spyware the likely number-one threat to network security in 2005. The poll showed that two thirds of IT managers and administrators believe that spyware will be the security threat that's going to keep them awake most nights this year. For more information, see: "Spyware likely top threat of 2005, but awareness lags: survey" at: http://www.integratedmar.com/ecl-usa/story.cfm?item=19129

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Increase	June 2004
3	Sober-I	Win32 Worm	Slight Decrease	November 2004
4	Zafi-D	Win32 Worm	Slight Decrease	December 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Bagle-AU	Win32 Worm	Stable	October 2004
7	Netsky-Z	Win32 Worm	Slight Increase	April 2004
8	Bagle.BB	Win32 Worm	Slight Increase	September 2004
9	Netsky-Q	Win32 Worm	Slight Increase	March 2004
10	Netsky-B	Win32 Worm	Return to Table	February 2004

Table Updated January 25, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Viruses or Trojans Considered to be a High Level of Threat**

  - Bropia.A: This worm spreads through the MSN Messenger and Windows Messenger instant messaging clients. The worm loads a keystroke logging Trojan horse, Rbot, and sends a copy of itself to all contacts in MSN Messenger and Windows Messenger instant messaging messaging client applications. Bropia.A is the latest indication that hackers and spammers no longer are content with spreading malware through e-mail. For more information see: http://www.newsfactor.com/story.xhtml?story_title=New-Worm-Piggybacks-on-MSN-Messaging&story_id=29934
  - Crowt-A: This worm poses as information on the latest news stories. It takes its subject lines, message content and attachment names from headlines gathered in real-time from the CNN website. Crowt-A's subject line and attachment share the same name, but continually change to mirror the front-page headline on the CNN news site. Crowt-A also installs a backdoor Trojan function. For more information see: http://www.sophos.com/virusinfo/articles/newsheadline.html
  - Gavno.a and Gavno.b: These two Trojan horse programs will render some Symbian-based mobile phones useless. Although almost identical with Gavno.a, Gavno.b contains the Cabir worm, which attempts to send a copy of the Trojan horse to other nearby Symbian-based phones via short-range wireless Bluetooth technology. The Gavno Trojans are the first to aim at disrupting a core function of mobile phones--telephony--in addition to other applications such as text messaging, e-mail, and address books. Gavno.a and Gavno.b are proof-of-concept Trojan horses that are not yet in the wild. For more information, see: http://www.pcworld.com/news/article/0,aid,119392,00.asp

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro,

Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Berbew.P	PWS-Dozat Trojan-Spy.Win32.Qukart.t	Trojan
Backdoor.Haxdoor.D	BackDoor-BAC Backdoor.Win32.Haxdoor.bg	Trojan
Cabir.N	-SEXY- EPOC/Cabir.N SymbOS/Cabir.N Worm.Symbian.Cabir.N	Symbian OS Worm
Cabir.O	EPOC/Cabir.O mobile SymbOS/Cabir.O Worm.Symbian.Cabir.O	Symbian OS Worm
Cabir.P	22207- EPOC/Cabir.P SymbOS/Cabir.P Worm.Symbian.Cabir.P	Symbian OS Worm
Cabir.R	EPOC/Cabir.R fuyuan SymbOS/Cabir.R Worm.Symbian.Cabir.R	Symbian OS Worm
Cabir.S	EPOC/Cabir.S guan4u SymbOS/Cabir.S Worm.Symbian.Cabir.S	Symbian OS Worm
Cabir.T	EPOC/Cabir.T iLoveU SymbOS/Cabir.T Worm.Symbian.Cabir.T	Symbian OS Worm
Cabir.U	EPOC/Cabir.U SEXXXY SymbOS/Cabir.U Worm.Symbian.Cabir.U	Symbian OS Worm
Downloader.Admincash	Trojan-Downloader.Win32.Small.ahk Trojan.Admincash Win32.BeavButt.A	Trojan
PWSteal.Formglieder		Trojan
PWSteal.Tarno.L		Trojan
Trojan.Mindos		Trojan
Trojan.Tannick.B	BackDoor-CAY BackDoor-CAY.dll Trojan-Spy.Win32.Agent.ao	Trojan
VBS.Rowam.A	I-Worm.Rowam.b VBS.Rowam VBS/Tiltel.B!Worm	Visual Basic Worm
VBS.Swerun		Visual Basic Worm
W32.Blatic.A		Win32 Worm
W32.Bropia	Bropia.A IM-Worm.Win32.VB.a W32/Bropia-A W32/Bropia.A.worm W32/Bropia.worm Win32.Bropia.A WORM_BROPIA.A	Win32 Worm
W32.Mirsa.A@mm		Win32 Worm
W32.Mydoom.AL@mm		Win32 Worm
W32.Mydoom.AM@mm	Email-Worm.Win32.Mydoom.ag MyDoom.AM W32/MyDoom-AM W32/Mydoom.AG.worm W32/Mydoom.AM@mm W32/Mydoom.AN@mm W32/Mydoom.av@MM Win32.Mydoom.AK WORM_MYDOOM.AM	Win32 Worm
W32.Nodmin@mm	Trojan.Win32.VB.ry	Win32 Worm
W32.Salga.B@mm		Win32 Worm
W32/Bobax-E	Trojan.Win32.Agent.aq WORM_BOBAX.F	Win32 Worm

W32/Crowt-A	Crowt.A W32.Crowt.A@mm W32/Crowt-A W32/Crowt.A.worm W32/Crowt.worm Win32/Crowt.A!Worm Worm.Win32.Cocoazul.e Worm/Crowt.A.DLL WORM_CROWT.A	Win32 Worm
W32/Forbot-DR	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-DS	Backdoor.Win32.Wootbot.am	Win32 Worm
W32/Kassbot-A	Backdoor.Win32.Delf.vb	Win32 Worm
W32/Kassbot-A	Backdoor.Win32.Delf.vb	Win32 Worm
W32/MyDoom-AL	W32.Mydoom.AL@mm W32/Mydoom.at@MM Worm/Wurmark.D.2.1 WORM_MYDOOM.AL	Win32 Worm
W32/MyDoom-AM		Win32 Worm
W32/Oddbob-C	Net-Worm.Win32.DipNet.f	Win32 Worm
W32/Rbot-TV		Win32 Worm
W32/Rbot-TW	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.y	Win32 Worm
W32/Rbot-UC	Backdoor.Win32.Rbot.ex	Win32 Worm
W32/Rbot-UD		Win32 Worm
W32/Rbot-UE		Win32 Worm
W32/Rbot-UH	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Sdbot-TQ		Win32 Worm
W32/Sdbot-TS	W32/Sdbot.worm.gen.h	Win32 Worm
W32/Sdbot-TV	Backdoor.Win32.SdBot.gen	Win32 Worm
W32/Sdbot-TW		Win32 Worm
Win32.Agobot.ANW	Backdoor.Win32.Agobot.gen Win32/Agobot.ANW!Worm	Win32 Worm
Win32.DedRunner.B	Trojan.Win32.Zapchast W32/Dedler.worm.dr Win32/Robobot.Trojan	Win32 Worm
Win32.DlCust.A	Troj/Dloader-FQ Trojan-Dropper.Win32.Small.pt Win32/Alureon.B.Downloader.Trojan	Win32 Worm
Win32.Lovgate.AX	I-Worm.LovGate.gen W32.HLLW.Lovgate.I@mm W32/Lovgate.w@M W32/Lovgate.W@mm Win32/LovGate.W.Worm	Win32 Worm
Win32.Mydoom.AJ	I-Worm.MyDoom.gen W32/Mydoom.at@MM Win32/Mydoom.AJ!Worm	Win32 Worm
Win32.Mydoom.AK	W32/Mydoom.gen@MM Win32/Mydoom.Variant!Worm	Win32 Worm
Win32.Palored.A	Trojan-Downloader.Win32.Murlo.a	Win32 Worm
Win32.Torp.A	Win32.Torp.A Win32/Torp.311296!Trojan	Win32 Worm
Win32.VideoDon.25092.A	Downloader-SS TrojanDownloader.Win32.Agent.cp Win32/VideoDon	Trojan
WORM_AGOBOT.AGK		Win32 Worm
WORM_AHKER.B		Win32 Worm
WORM_NODMIN.A		Win32 Worm
WORM_RBOT.AIW		Win32 Worm
WORM_WURMARK.D		Win32 Worm

[back to top]

Last updated January 26, 2005